Comparison of hardware firewalls in a network environment

Mälardalens Högskola
School of Innovation, Design and Engineering
Albin Elnerud
Aed07004@student.mdh.se
Bachelor of Science in Engineering - Computer Network Engineering
17/5-2017
Examiner: Mats Björkman
Supervisor(MDH): Elena Lisova
Supervisor(MDH): Jakob Danielsson
Supervisor(Eskilstuna): Jimmy Sjöberg
Abstract

Today's market offers a wide range of available firewalls, there are many manufacturers and each of them has at least several series of possible solutions. As organisations and companies seek to protect their assets against current and new hostile threats, the demands for network security increases and drives the development of firewalls forward. With new firewall technologies emerging from a wide variety of firewall vendors, choosing the right firewall can be both costly and time consuming. Requirements for a concrete network are needed to be correlated with security functionalities, i.e., metrics for firewalls. Incorrect requirements formulation or their incorrect mapping to metrics can lead to a financial loss or a firewall failure in providing desired security functionalities. In this thesis, firewalls from three different manufacturers are investigated. Firewalls are compared and evaluated by using requirements derived for Eskilstuna municipals network. To identify solutions fulfilling the requirements, metrics related to the requirements are identified. Two different placements for firewall deployment are considered separately, as they have different requirements. The firewall comparison consists of two steps. The first step of the comparison is done by evaluating firewalls from each manufacturer separately. After the best suited firewall from each manufacturer has been identified, the second step in the comparison is performed. The step two consists of comparing the best solution from each manufacturer between each other. The outcome of the comparison is a firewall solution that fulfills all requirements and can be considered as optimal choice for the investigated network environment.
1 Background and motivation

Security, defined in the English Cambridge dictionary as “protection of a person, building, organization, or country against threats such as crime or attacks...” [1], is an important topic that concerns us all in our everyday life, whether we realize it or not. Security can be a protection against a theft imposed by different security policies and achieved by using simple locks to keep away unauthorized intruders. In computer networks, security has become more technical due to the challenges we face today (e.g., an adversary can perform an attack just by using a computer with an internet access), but still has the same overall goal, i.e., to provide protection against threats. The NIST Risk Management Guide states that “a threat is the potential for a particular threat-source to successfully exercise a particular vulnerability”, where a vulnerability can be defined as “a weakness that can be accidentally triggered or intentionally exploited” [2].

A need for secure communication in the internet may never have been more urgent than it is today, as sensitive information often can be stored on public servers [3]. Particular security solutions tightly depend on specific applications. For example, to assure that the information is kept securely, one can use a password for authentication or a more complex access control method such as Authentication, Authorization and Accounting (AAA), which controls computer resources available to a user to access [4]. The first essential step in an efficient security implementation is identification of security specifics that are needed. For instance, if too strict rules are set in place it could remove the usability and accessibility of the requested material for the intended users. On the contrary, too soft rules may instead allow unwanted and hostile traffic to be present in the network.

In the most extreme case, to guarantee full security of a specific resource, its access could be completely shut off. However, doing this would fully eliminate accessibility of the resource and make it useless. Although, the aim is to achieve the highest level of security to protect the resource, disregarding its availability would be contra productive. A compromise between how secure one wants the network to be and its usability, is an aspect to take into consideration when choosing and implementing network security solutions. A successful implementation of a security solution implies that all specified requirements are met. Requirements can be defined as “technical features (e.g., access controls), assurances (e.g., background checks for system developers), or operational practices (e.g., awareness and training)” [5]. Requirements are derived from a number of sources including laws, policies, guidelines and functional needs of a considered system [5].

In network security, firewalls are one of the techniques to provide security functionalities for a network. A firewall is placed between a secure zone inside the network and an unsecure outside zone. It acts as a security door between the two entities by allowing internet traffic from the inside network to pass to the outside network, and restricting outside traffic from entering the inside network. A firewall decides which traffic is allowed to traverse between the boundaries by inspecting where the traffic is originated from and also by examining its content. By enforcing different policies the firewall decides based on different criteria if access should be granted for traffic or not. The firewall can be a determining factor in security depending on a configuration and established rules, by either providing strong defence or adding vulnerabilities to the network if configured wrongly.

Different firewall manufacturers offer a span of different techniques and predefined rules bundled together in licenses. Corporations can buy and implement those licenses in their network. Choosing which kind of firewalls fits into a specific network can be a tedious process considering the range of different functionalities and offers from manufacturers. Poor optimization of a firewall can lead to an excessive complexity, a weak access control, security
risks and performance degradation etc. These factors lead to a loss for the corporation owning the network [6]. A firewall is an important part of network security, however it also has other functions that may enhance the network from a non-security point of view, e.g., properties related to fault tolerance [7] and address translation [8].

2 Firewalls
Different generations of firewalls are often referred to when discussing firewall development through the time [9], [10]. A firewall generation consists of several types of firewall technologies that have evolved to meet the demands on network security relevant at a particular period of time. Technologies are moving forward with development of new systems and approaches, correspondingly the amount of possible ways that adversaries can use to exploit the new technologies increases as well. The development of firewalls continues to evolve in order to meet new arising threat challenges.

2.1 OSI model
The Open System Interconnection (OSI) model was developed to overcome the problem arising from different computer manufacturers using their own set of conventions to interconnect equipment. The International Organization for Standardization (ISO) recognized the need for standards for connecting heterogeneous informatics networks and presented the OSI reference model [11]. The OSI model is composed of seven layers where each layer represents a group of related network functions. Once communication between networked computers occur, each layer is traversed descending from the sending computer and ascendingly to the receiver. In network security the OSI model can be used to explain where different security features operates. Traditionally, layer two, three and four have been used in network security regarding firewalls. It is no longer the case as firewall security solutions now include all layers from two to seven.

- Layer 1, Physical. Specifications regarding electrical, mechanical, procedural and functions for activating, maintaining and releasing physical connections.
- Layer 2, Data Link. Provides error-free transfer of data frames between connections over the physical layer.
- Layer 3, Network. Provides routing and related functions to control what path data should take based on logical addressing.
- Layer 4, Transport. Implements data transport services to ensure the messages are delivered error-free, in sequence and without data loss.
- Layer 5, Session. Establishes, coordinates and terminates communication connections.
- Layer 6, Presentation. Formats or translates data to be used by the application layer.
- Layer 7, Application. Enables users or applications to process network services such as identifying communication partners, determining network capacity and synchronizing communication.

The layers in the OSI model are continually referred in firewall characteristic explanations.

2.2 Different types of firewalls
As of today, there exist many different types of firewalls with different technologies. Each type of firewall often has one or more properties which distinguishes themselves from the other
types of firewalls. This section presents a brief overview of the key functionalities of some of the most common types of firewalls.

2.2.1 Basic packet filtering
A packet filter firewall operates mainly at layer two and three of the OSI model. The decisions made by the firewall for the targeted packets are based on a predefined ruleset. For each packet received by the firewall, the decision is made depending on the packet type (UDP, TCP, etc.), source and destination IP address, source and destination ports. By allowing or denying the packet the firewall provides basic network access control. Another name for the packet filtering firewall is a stateless firewall, which refers to the firewall inability to control a state of the connection between sender and receiver, as packets are processed as single units without regard of related packets [8].

2.2.2 Stateful firewall
A stateful firewall has the same capabilities as a packet filter firewall but with an additional ability to monitor and store session and connection states. According to the OSI model, layer four deals with these states. The firewall can determine whether a packet belongs to the same connection by associating related packets based on source and destination IP addresses, source and destination ports and the protocol used. With the ability to monitor connections the firewall can take actions to prevent packets that deviate from the expected state to enter the network [8].

2.2.3 Circuit level firewall
Similar to a stateful firewall, a circuit level firewall monitors a session state. However, the firewall also introduces an ability to prevent direct connections between hosts on the opposite side of the firewall. The firewall acts as an intermediary between two hosts and simulates a direct connection between the two. This is achieved by translating ports and addresses, also called Port Address Translation (PAT) and Network Address Translation (NAT). Firewalls that have NAT and PAT, can hide host addresses from the public and translate the hidden addresses into public ones if a valid (based on the firewalls ruleset) connection request is initiated [12].

2.2.4 Application firewall
An application firewall introduces an ability to work on the seventh layer in the OSI model and inspects the traffic content. Unlike stateful firewalls, which can track the type of traffic based on the used port, application firewalls examine the traffic and can verify the application that the traffic is constituted of. This gives the firewall means to stop malicious traffic that hide behind other protocols and ports [8].

2.2.5 Virtual firewall
A physical firewall can be partitioned into several logical instances. Each instance acts and behaves as a standalone firewall with its own configuration and security policy. With the ability to create logical instances, different physical parts of a network can be segmented into logical parts each of which has its own security policy [13].
2.3 High availability
High availability (HA) allows firewalls to be placed together in a group sharing a synchronized configuration in order to prevent single point of failure. In a HA group of two firewalls, if one firewall stops working, another firewall overtakes the responsibilities of the failed firewall. HA can be configured in two ways: active/active and active/standby (passive).

According to an active/standby configuration, one firewall manages all traffic while the second firewall is continuously synchronized. If the active firewall fails, the passive firewall takes over without interruption in the traffic. In an active/active configuration, both firewalls in the group are actively processing traffic. If failure on any of the firewalls occur, the other firewall takes over all traffic [14].

2.4 Next generation firewalls (NGFW)
As threats continue to evolve, new security solutions arise and traditional firewalls can no longer provide the necessary protection to a network. Next Generation Firewalls (NGFW) incorporates different security solutions into one compliance while still performing functionalities of a traditional firewall. There is no formulated standard for what NGFW has to include to be called NGFW. However, Gartner released a definition in 2009 [15] of what NGFW should include:

- Application Awareness and Full Stack Visibility
- Integrated IPS
- Extra-Firewall Intelligence
- Standard first generation firewall features

In 2016 NSS labs defined the requirements for NGFW as [16]:

- Application awareness/control
- User/group control
- Integrated intrusion prevention system (IPS)
- Ability to operate at Layer 3 (“traditional”)
- External intelligence to enhance blocking decisions (i.e., “reputation services”)
- Anti-malware
- SSL inspection ability
- Traditional “first generation firewall” features

2.4.1 Application awareness and full stack visibility
This property refers to a situation, when a firewall can identify the traffic type regardless of the port, protocol, encryptions or other evasive tools. This is accomplished by scanning every byte of the packets payload, comparing the payload information with predefined matching patter and then identifying the traffic type based on the matched pattern.

2.4.2 Integrated intrusion prevention system (IPS)
The IPS is a tool that monitors traffic activities of malicious or unwanted behaviour and takes actions based on a predefined configuration. Malicious or unwanted behaviour can be related to malware, unauthorized access attempts or privileges misuse. When undesired traffic is encountered the IPS can react and block the traffic from entering the network. Following the block, notification and detailed report of the violation give a security administrator a detailed
view of traffic violations in the network. IPS techniques have been a part of network security but used as a standalone unit next to the firewall. In NGFW, IPS is now integrated in the firewall as an embedded solution.

There are three main detection methods used in IPS. The first one is signature based that uses predefined threat patterns. The next one is anomaly based that can detect traffic behaviour that deviates from the normal. Finally the last one is stateful protocol analysis that uses profiles that specify how specific protocols should be used [17].

2.4.3 Extra-firewall intelligence or user/group control
User and group control is a mechanism helping to control the use of applications and network resources based on a user demanding it. By linking IP addresses to user identities, control over user activities on the network is achieved. The linking between IP addresses and users is supported with a help of directory services such as Active Directory (AD) [9].

2.4.4 External intelligence to enhance blocking decisions
One of the ways to enhance access permission decisions is referring to external sources to keep the threat database updated with most recent attacks and compromises. Firewall vendor continually updating the threat software, which allows firewalls to take actions against attacks according to a current state-of-the-art [18].

2.4.5 SSL inspection ability
Secure Socket Layer (SSL) is a broadly used internet protocol for secure communication. By using it together with hypertext transfer protocol (HTTP) it is possible to encrypt traffic over the World Wide Web. This encryption allows web hosts and web servers to communicate securely over an open communication media [19].

As a response to increased use of SSL encryption in the internet, attacks were found hiding in SSL traffic. Firewalls with a SSL inspection can decrypt the encrypted SSL traffic, analyse the content and then re-encrypt the traffic and forward it to the destination.

2.5 Firewall placement
A firewall can be placed at different locations in a network. Placement at the logical border of a network as is showed Figure 1, is generally the most common way of placement. A firewall at the border is located between the outside network (most commonly internet) and the inside protected network.

![Figure 1- Firewall on the border](image-url)

A firewall can also be placed inside the network as shown in Figure 2, where one firewall is on the border and one is inside the network.
In Eskilstuna municipals network, one firewall is placed at the border. This firewall requires a high level of security as it serves as a primary defence for the protected network. One firewall is also placed inside Eskilstuna municipals network and is used to segment different parts of the network into separated instances. This firewall is more focused on rules and regulations for different user groups and not on inspecting traffic. It does not require the same level of security that the firewall on the border does.

3 Problem formulation

Firewalls play a crucial role in today’s network environment by providing security functionalities on a border of zones with restricted and unrestricted access [8]. Corporations have different options for choosing a firewall manufacturer and its configuration. There is a difference in functions and pricing as each manufacturer uses its own technics and software. The firewalls features are also bundled together in licenses that are sold to companies as complete products. Therefore, if needed security functionalities are not defined properly, it may result in the company buying functionalities it might not need. A comparison between manufactures firewall offers can create underlying material to distinguish the differences. There are several steps to implement a firewall solution [22], and implementation errors may increase the possibility of vulnerabilities exploitation by an adversary. The result of such exploitation can be money loss [23], data leakage and damage of intellectual property [24]. To minimize security risks, security requirements regarding firewalls in corporate networks are needed to be examined. An evaluation of existing firewall solutions is required to understand which requirements in networks are necessary and which firewall functionalities can be provided by different manufacturers. The results provide information on how to enhance usage of firewalls and identify existing gaps between network requirements and firewall solutions.

The formulated problem can be addressed by answering the following research questions:

- RQ1: Which security solutions can be provided by firewall functionalities?
- RQ2: What are the differences between firewalls produced by different manufacturers?
- RQ3: What requirements are there for firewalls in a corporate network environment?
- RQ4: How can the derived requirements be met by means of the considered firewalls?
4 Methodology

A number of approaches are used in this research in order to answer the formulated research questions. The methodology flow can be presented by the following steps.

4.1 Data gathering and analysis

The thesis uses existing researches and studies regarding firewalls in order to identify security metrics. The metrics are firewall features that can be used to satisfy specified network requirements.

4.1.1 Literature review

The review is conducted over firewall functions and techniques in order to answer RQ1 and RQ2. Along with the input from the company, the review also partially answers RQ3. Considered literature regarding specific functions of firewalls have its main focus on three of the biggest leading manufacturers of hardware firewalls, namely, Cisco, Checkpoint, Juniper. Papers from other researchers related to the topic are used to build a general literature review. Technical documents from the manufacturers are reviewed for more technical details.

The following resources are used in the thesis:

- IEEE Xplore® Digital Library, IEEE Xplore provides web access to more than four-million full-text documents from some of the world’s most highly cited publications in electrical engineering, computer science and electronics\(^1\).
- Google Scholar, indexes full text or metadata of scholarly literature and includes academic journals, theses, technical reports and more\(^2\).
- Cisco Systems Inc. Firewall manufacturer\(^3\).
- Check Point software technologies LTD. Firewall manufacturer\(^4\).
- Juniper Networks. Firewall manufacturer\(^5\).

4.1.2 Metric identification

To be able to evaluate firewalls and answer RQ2, a comparison between three firewall manufacturers is conducted. The comparison is performed by using a set of metrics. These metrics come from literature review and input from an Eskilstuna municipality representative. By dividing the metrics in two groups related to security and general ones, we can separate general needs which do not have a direct connection with security from security functionalities.

Below is a list of metrics identified based on the literature review.

General metrics
- Fault tolerance support
- Connection throughput

---

\(^1\) [http://ieeexplore.ieee.org/Xplore/home.jsp](http://ieeexplore.ieee.org/Xplore/home.jsp)
\(^2\) [https://scholar.google.com/](https://scholar.google.com/)
\(^3\) [http://www.cisco.com/](http://www.cisco.com/)
\(^4\) [https://www.checkpoint.com/](https://www.checkpoint.com/)
4.2 Requirements derivation
A representative of Eskilstuna municipality, Jimmy Sjöberg, has provided requirements for firewalls based on Eskilstuna municipality’s specific needs. The requirements formulated by Eskilstuna municipally are used to protect the company’s assets. An asset can be defined as “an object or resource which is “worthy” enough to be protected” and can be physical equipment (e.g., computers), data (e.g., files) or software (e.g., configuration files) [25]. The requirements may also include aspects that do not provide any protection for assets, but are or importance for the company, e.g., price of the equipment and processing capacity.

The set of requirements is complimented by an outcome of literature review. The review is done to get a broader picture of firewall requirements, i.e., requirements that are not considered by Eskilstuna municipality. The overall outcome is a set of security requirements that should be met in order to provide required level of assets protection, and requirements that met general non-security related needs of the company. The gathered requirements are used to answers RQ3.

4.3 Evaluation
Based on derived metrics and requirements, an evaluation is done to answer RQ4. The evaluation is done by mapping identified firewall metrics with the derived network requirements. A way to optimize a firewall usage is developed by identifying the gaps between firewall solutions and network requirements.

5 Related works
Previous works comparing firewalls that can be found in literature often focus on software based firewalls and only to some extend on hardware firewalls [26]-[30]. S. Patton et al. [26] made a comparison of a Cisco 2621 router with a firewall Internetwork Operating System (IOS) and an open source Redhat 6.0 Linux operating system on a Pentium microcomputer. It provided analysis between an open source firewall code and a proprietary firewall code by comparing Virtual Private Network (VPN) capabilities and a firewall feature called application level filtering. Application level filtering enables the firewall to make decisions related to traffic based on the application that is used, i.e., File Transfer Protocol (FTP) or Simple Mail Transfer Protocol (SMTP). The comparison is done by measuring the performance during data transfer with the conclusion that a combination of two firewalls may be the optimal solution for the considered VPN and Application level filtering metrics. In another comparison three different firewalls, namely, Cisco ASA, Checkpoint SPLAT and OpenBSD PF, were analysed in terms of
their performance [28]. The authors have measured the performance of the firewalls by comparing throughput of different internet protocols. A comparison of security functionalities was as well presented in the same report with the help of an application called NetWag, an open source application that can be used to test different security aspects of a firewall. The results show that the Cisco firewall had better performance in terms of throughput capacity and all three demonstrated basic security capabilities, such as preventing unwanted traffic from entering the network. The two works described above show how comparisons of firewall security functionalities and performance can be done through tests with different measurements. In this thesis measurements of different metrics considered for the comparison are obtained from tests done by the firewall manufacturers and independent studies. The measurements allow to derive a wider variety of comparison metrics to identify the differences between firewalls.

A comparative study for five firewalls in a specific test environment was done by C. Niklasson and C. Lindström [29]. Two of them were hardware firewalls with Cisco software, Cisco 2801 router and Cisco ASA 5510 firewall, and the rest three were software based firewalls, Iptables, Mikrotik and Windows 2003 server. The hardware firewalls demonstrated better results in such tested aspects as security and throughput. In this thesis only hardware firewalls are considered.

T. Höffler et al. conducted a more in depth comparative study [27], the following firewalls were considered, OpenBSD PF, IP Tables, Windows 2003 server, SunScreen 3.2 and IP Filter. The five software firewalls were tested regarding their security properties by conducting various network attacks against them, and regarding their performance properties by rating throughput, latency and a limit for simultaneous connections. The result was ambiguous and none of the firewall could outperform the others in all tested aspects. When comparing firewalls, diverse criteria are needed to identify the differences between firewalls. In the described above work different firewall requirements were used to establish criteria for the comparison. In this thesis metrics related to firewall features are used as comparison criteria.

S. Persson and A. Malmgren [30] completed a study regarding two firewalls, Juniper SRX1500 and Palo Alto PA-3020. The study examined which of the two firewalls suits the expanded network of the targeted company based on its future requirements. The derived requirements were used together with a list of testing guidelines to evaluate the firewalls. The evaluation resulted in a recommendation towards PA-3020 being used as a solution for the network. The described approach is similar to the method used in this work, however in the thesis firewall features are considered as comparison metrics instead of testing guidelines. Moreover, a different set of requirements is used for the evaluation in order to meet specific firewall needs.

6 Requirements

A firewall can provide various functionalities depending on a concrete use case. One reason for a particular configuration can be a need to maintain access control over Internet Protocol (IP) packets for a designated network. Another reason can be to provide a secure way for users to access sensible data. Therefore, the demands on firewalls are not always the same in all use cases. In order to meet the demands and achieve the desired functionalities for firewall solutions, it is crucial to define requirements.

The firewall requirements that are specified by an organization or a company, should also fit into the overall security policy. A firewall should not be viewed as a standing aside independent security solution, but as a complement to the organization security.
The requirements specify necessary security and general functionalities that should be provided by a firewall. In order to derive requirements it is important to identify firewall limitations.

The following two requirements are requirements that depend on an implementation and an environment of the firewalls. They are non-functional requirements and are used as recommendations or guidelines for a possible implementation.

**Special requirement 1**
All traffic must go through the firewall [27].

- In order for the firewall to maintain its functionality, all traffic that is to be inspected, regulated or monitored in some way, shall go through the firewall. If the traffic is not traversing the firewall no action or control can be taken from the firewall. Firewalls are often placed between the organizations network and the public network (internet). If other connections between the two networks are in place, traffic that is intended to be inspected by the firewall, can circumvent and dodge the firewall control.

**Special requirement 2**
The firewall must provide the desired functionality [8].

- The purpose behind acquiring and implementing a firewall can be on different grounds. Some organizations require the best available security with the latest features on the firewalls, while others only require basic firewall security. It is necessary to evaluate what the firewall is supposed to contribute to the network in order to attain the desired function of the firewall. After the firewall is configured and placed in the network, the firewall must be able to fulfil those sought needs.

The requirements presented in the rest part of this section are provided by Eskilstuna municipally. The requirements can be divided into security and general requirements. Requirements with security focus should comply with a security policy of the company. Requirements from the general group assure that other network and company demands are met. Some of the requirements have concrete numbers and some are generally described. Following Eskilstuna municipals network needs, two types of firewalls, described in section 2.9 are considered separately as different requirements are relevant for them. The outside firewall that is placed on the border, is hereafter referred as F1, the inside firewall is hereafter referred as F2.

**Requirement 1 (R1): protection**
The firewall (F1) shall provide protection against network attacks.

- Threat detection and attack mitigation shall provide security for the organization network. The threats and attack include but are not limited to spoofing attacks, man in the middle attacks and malware. In order to keep the network secure, the firewalls ability to detect threats and deter attacks is crucial.

**Requirement 2 (R2): performance**
The firewall (F1, F2) shall have the capability to handle all user data and connections.
All user communication over the network shall be satisfied. Thus, data transfer and network usage cannot be hampered by the firewall. If the firewall does not meet the required network performance specifications, bottleneck of traffic may become a problem. The firewall must also have the capacity to perform its security functions within acceptable time for a considered network size and a user base. The minimum connection throughput required is 2GB/s. The amount of new connections per second required is 25,000. Number of required concurrent connections is 100,000.

**Requirement 3 (R3): 24/7 uptime**
The firewall (F1, F2) shall never stop.

– Attacks can happen at any given time, therefore the firewall shall have the same capabilities day and night. If the firewall for any reason stops working, the network becomes compromised. The firewall shall also never be a reason to network downtime due for firewall failure.

**Requirement 4 (R4): virtual firewall**
The firewall (F2) shall support virtual segmentation.

– In any organization it can be necessary to separate users into instances with different security and access levels. Virtual segmentation enables such a separation within the network. A support of minimum 20 different virtual instances is required.

**Requirement 5 (R5): price**
Total cost of the firewall (F1, F2) shall be the lowest possible.

– The firewall should be within the organizations budget while still performing the required functions. The cost is not always a onetime payment but a continuation over a period of time.

The table below summarizes presented above requirements.

<table>
<thead>
<tr>
<th>ID</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>protection</td>
</tr>
<tr>
<td>R2</td>
<td>performance</td>
</tr>
<tr>
<td>R3</td>
<td>24/7 uptime</td>
</tr>
<tr>
<td>R4</td>
<td>virtual segmentation</td>
</tr>
<tr>
<td>R5</td>
<td>price</td>
</tr>
</tbody>
</table>

*Table 1 - Requirements*

7 **Metrics**

In this section metrics are reviewed. The metrics are used to assure company requirements fulfilment and serve as comparison grounds. One requirement does not always correlate to one metric and thus there can be several metrics related to the same requirement. The documentation from the firewall manufacturers and the input from the company are used to identify the metrics.
R1: Protection
In order to provide the necessary protection discussed in R1, the four following metrics are used:
- Metric 1 (M1), Internet filter with updated classifications.
- Metric 2 (M2), User identification and control.
- Metric 3 (M3), Ability to prioritize traffic based on users and applications.
- Metric 4 (M4), Malware protection.

R2: Throughput
The firewalls shall be able to handle a desired connection throughput to match the company’s internet connection speed and have the capacity to serve the company’s users.
- Metric 5 (M5), Connection throughput.
- Metric 6 (M6), Concurrent connections.
- Metric 7 (M7), New connections per second.

R3: 24/7 uptime
In order to satisfy R3, HA solutions are investigated.
- Metric 8 (M8), HA.

R4: Virtual segmentation
The firewall shall support virtual instances.
- Metric 9 (M9), Virtual instances.

R5: Price
The firewall price is considered within this thesis only as a market price to buy a considered firewall. Therefore, the price for its configuration and maintenance is not considered as these factors are tightly connected with a concrete use case.
- Metric 10 (M10), Price.

Table 2 summarizes the metric to requirement correlation.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1, M2, M3, M4</td>
<td>R1</td>
</tr>
<tr>
<td>M5, M6, M7</td>
<td>R2</td>
</tr>
<tr>
<td>M8</td>
<td>R3</td>
</tr>
<tr>
<td>M9</td>
<td>R4</td>
</tr>
<tr>
<td>M10</td>
<td>R5</td>
</tr>
</tbody>
</table>

Table 2 - Metrics and requirements

8 Comparison
In the subsections 8.1-3, a comparison of each manufacturers firewall supply is conducted to find the best suited firewall from each manufacturer. A price as a metric is considered separately in the subsection 8.4. Next, in the subsection 8.5 a comparison between the
manufacturers is presented with individual tables for F1 and F2. Finally, 8.6 contains a short research report about NGFW performances.

In order to consider a firewall, all requirements which correlates to Special Requirements 2 shall be met. The metrics are used to check that the firewall has the required functionality to fulfil a requirement. If a metric have a value, a comparison of the value is conducted. All material used in the comparison is taken from respective manufacturers documentation [31],[32],[35]-[39]. Each firewall has a model number that is used to differentiate the firewalls from the same vendor. A higher model number within each vendor corresponds to more powerful firewall hardware.

8.1 Checkpoint

The Checkpoint firewall security appliances are divided into Small Office Series, Branch Office Series, Small Enterprise Series, Midsize Enterprise Series, Large Enterprise Series and Data Centre Series. Each series consists of one or more firewall versions designed to match networks of different sizes. Table 3 is snipped from Checkpoint’s documentation regarding performance, where selected models from Small Office to Midsize Enterprise series are shown.

<table>
<thead>
<tr>
<th>Model</th>
<th>Performance</th>
<th>2200</th>
<th>3100</th>
<th>4800</th>
<th>5100</th>
<th>5200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput (Gbps)</td>
<td></td>
<td>3</td>
<td>4</td>
<td>11</td>
<td>14.5</td>
<td>16</td>
</tr>
<tr>
<td>Connections Per Second(K)</td>
<td></td>
<td>25</td>
<td>40</td>
<td>70</td>
<td>110</td>
<td>125</td>
</tr>
<tr>
<td>Concurrent Sessions(M)</td>
<td></td>
<td>1.2</td>
<td>3.2</td>
<td>3.3</td>
<td>3.2</td>
<td>3.2</td>
</tr>
</tbody>
</table>

Table 3 - Checkpoint Performance

All the above firewalls fulfil R2 by all three metrics. Table 4 shows a list of security suits available to the firewalls series.

<table>
<thead>
<tr>
<th>Model Series</th>
<th>NGFW</th>
<th>NGTP</th>
<th>NGTX</th>
</tr>
</thead>
<tbody>
<tr>
<td>2200</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>3000</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>4000</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>5000</td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Table 4 - Checkpoint Model Series NGFW solutions

In order to satisfy R1 the metrics M1, M2, M3 and M4 are considered and are fulfilled by Checkpoints NGFW solution. Next Generation Threat Prevention (NGTP) and Next Generation
Threat Extraction (NGTX) are Checkpoint’s new versions of NGFW with updated functionalities. Checkpoint ClusterXL software solution allows firewalls to achieve redundancy with High-Availability. ClusterXL also allows for firewalls to become a virtual group (cluster) that acts as a single physical unit. Checkpoint ClusterXL software is available to all firewalls suits.

Virtual systems are Checkpoint virtual firewall solution. A minimum of 20 virtual instances is required to satisfy R4. Checkpoint 5000 series offers a maximum of 20 virtual instances and only firewall 4800 in the 4000 series offers more than 20(25). The large enterprise series and Data Centre series offer from 40 to 250 virtual instances. Table 5 shows a few of the considered firewalls virtual system capacity.

<table>
<thead>
<tr>
<th>Model</th>
<th>2200</th>
<th>3100</th>
<th>4800</th>
<th>5100</th>
<th>5200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Systems</td>
<td>3</td>
<td>10</td>
<td>25</td>
<td>20</td>
<td>20</td>
</tr>
</tbody>
</table>

Table 5 - Checkpoint Virtual Systems

8.2 Juniper

Junipers firewall appliance consists of Branch Series for small and medium sized networks, and Infrastructure Series for medium and large network environments. Table 6 shows the Branch Series firewalls performance.

<table>
<thead>
<tr>
<th>Model</th>
<th>SRX240</th>
<th>SRX550</th>
<th>SRX650</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance</td>
<td>Throughput (Gbps)</td>
<td>1.8</td>
<td>7</td>
</tr>
<tr>
<td>Connections Per Second(K)</td>
<td>8.5</td>
<td>27</td>
<td>35</td>
</tr>
<tr>
<td>Concurrent Sessions(K)</td>
<td>256</td>
<td>375</td>
<td>512</td>
</tr>
</tbody>
</table>

Table 6 - Juniper Performance

Firewall SRX550 and SRX650 both satisfy R2 through M5. SRX550 and SRX650 are also the only ones in Branch Series to meet R2 through M7 and M8. All firewalls in the Infrastructure Series satisfy R2 through all metrics. Junipers NGFW solution is available to all Juniper models and satisfies R1 through all related metrics. In Juniper SRX firewall series Junos Service Redundancy Protocol (JSRP) allows an HA configuration with two hardware identical firewalls. The HA solution satisfies R3 through M8.

Junipers Logical System enables SRX firewalls to be partitioned into contexts. Logical System is only available to a few firewalls within the Infrastructure Series, SRX3400, SRX3600, SRX5600 and SRX5800. R4 specifies a minimum of 20 logical instances, Junipers Logical System allows up to 32.
8.3 Cisco
Cisco's ASA 5500-X firewall series targets Small offices, Branch locations and Internet-edge deployments. The throughput of the 5500-X series firewalls is shown in Table 7.

<table>
<thead>
<tr>
<th>Model Performance</th>
<th>ASA5515</th>
<th>ASA5525</th>
<th>ASA5545</th>
<th>ASA5555</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput (Gbps)</td>
<td>1.2</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Connections Per Second(K)</td>
<td>15</td>
<td>20</td>
<td>30</td>
<td>50</td>
</tr>
<tr>
<td>Concurrent Sessions(M)</td>
<td>0.25</td>
<td>0.5</td>
<td>0.75</td>
<td>1</td>
</tr>
</tbody>
</table>

*Table 7 - Cisco Performance*

The 5525-X model meets R2 requirements through M5 and M6 but not by M7. The next model, 5545-X meets all demands for R2. The Cisco NGFW solution is available to all firewalls in the 5500-X series and meets the demands on R1 by all metrics. The firewalls from Cisco support HA on all firewalls in the 5500-X series.

Security context allows Cisco firewalls to be used as virtual devices and make them similar to multiple stand-alone devices. The minimum number of security contexts for R4 is 20 and is met by 5525-X, 5545-X and 5555-X as shown in Table 8.

<table>
<thead>
<tr>
<th>Model Security contexts</th>
<th>ASA5515</th>
<th>ASA5525</th>
<th>ASA5545</th>
<th>ASA5555</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>20</td>
<td>50</td>
<td>100</td>
</tr>
</tbody>
</table>

*Table 8 - Cisco Security Contexts*

8.4 Price
There is no list of prices for the firewalls on vendor's websites. The manufacturers recommend buyers to contact certified resellers in the respective country for purchase. The price is not always listed on the reseller's documentation for offers, and it is often required to take direct contact to determine the price for a firewall unit. Virtual Graffiti [33] is a partner with the tested firewall vendors. They provide price lists for most products and their data is used in the comparison. What can be concluded is that a firewall price increases with each model version. The lowest price for each manufacturer is thus the firewall with the lowest model number. As the lowest price is wanted and the price goes down with each firewall model, the firewall that meets all the requirements and has the lowest model number is considered in this thesis as the best solution from each vendor.

8.5 Comparison between vendors
In the comparison between vendors, the firewall that matches the minimum requirement and has the lowest model (because of the price) in the series is chosen. In regards of a possible
expansion of the network, if a firewall that is considered meets the requirements with the exact number, the next model in the series is also listed. Table 9 and 10 present the comparison between the firewalls.

<table>
<thead>
<tr>
<th>F1</th>
<th>Metric</th>
<th>Checkpoint</th>
<th>Checkpoint</th>
<th>Juniper</th>
<th>Cisco</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2200</td>
<td>3100</td>
<td>SRX550</td>
<td>ASA 5545</td>
<td></td>
</tr>
<tr>
<td>1/2/3/4</td>
<td>Y/Y/Y/Y</td>
<td>Y/Y/Y/Y</td>
<td>Y/Y/Y/Y</td>
<td>Y/Y/Y/Y</td>
<td></td>
</tr>
<tr>
<td>5/6/7</td>
<td>3/25k/1,2m</td>
<td>4/40k/3,2m</td>
<td>7/27k/375k</td>
<td>3/30k/750k</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>$3,188.00</td>
<td>$6,038.00</td>
<td>$9,500.00</td>
<td>$12,379.00</td>
<td></td>
</tr>
</tbody>
</table>

Table 9 - Firewall 1 comparison

<table>
<thead>
<tr>
<th>F2</th>
<th>Metric</th>
<th>Checkpoint</th>
<th>Checkpoint</th>
<th>Juniper</th>
<th>Cisco</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5200</td>
<td>4800</td>
<td>SRX3400</td>
<td>ASA 5545</td>
<td></td>
</tr>
<tr>
<td>5/6/7</td>
<td>16/125k/3,2m</td>
<td>11/70/3,3m</td>
<td>30/150k/2,25m</td>
<td>3/30k/750k</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><strong>20</strong></td>
<td>25</td>
<td>32</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>$9,258.00</td>
<td>$20,528.00</td>
<td>$17,100.00</td>
<td>$12,379.00</td>
<td></td>
</tr>
</tbody>
</table>

Table 10 - Firewall 2 comparison

8.6 NSS Labs

NSS Labs is an independent information security research and testing organization. They provide unbiased data for various security products. A report on security effectiveness, performance and total cost of ownership on NGFWs released in 2016 is shown in Figure 3. Juniper Networks SRX5400E, Check Point 13800 and Cisco ASA 5585-X SSP60 were among 13 tested products. In the graph in Figure 11, Security Effectiveness and Total Cost of Ownership (TCO) per protected Megabits per second (Mbps) are presented. TCO is the cost over a three year period and includes initial acquisition, deployment, maintenance and update cost. Juniper, Checkpoint and Cisco all received a high score in security effectiveness. Juniper placed much higher than Cisco and Checkpoint on the TCO scale with $97 followed by Cisco $51 and Checkpoint $25 [34].
9 Discussion

The comparison between the three manufacturers shows that they all have a number of firewalls that could satisfy the requirements. A point to note in the comparison is the disregard of everything else than what is specified in the requirements. Even though, other considerations such as a reliable hardware support and a location of resellers can be of importance.

In the comparison, the throughput requirement expressed through the metric $M_5$, connection throughput was investigated based on the documentation by each firewall throughput in ideal testing conditions. There are also other throughput measurements obtained with extra firewall features turned on. Some of these features also have an impact on the performance throughput and should be taken into consideration. However, as the requirement only specified connection speed and not the entire throughput capacity of the firewall, this is left out of the thesis.

NGFW solutions for all vendors are highly prioritized and well supported. All NGFW solutions include a high standard on security functionalities and have the requested features. All considered vendors are also evaluated high in the NSS labs report regarding security.
effectiveness, which indicates a good understanding of NGFW requirements and threat prevention.

An interesting observation regarding redundancy can be made, all vendors consider it as an important topic. This is reflected by their High-availability solutions that are available for all examined firewalls.

The requirement for firewall virtual instances is satisfied with model 5200 and model SRX3400 from Checkpoint and Juniper respectively. Both with stronger hardware and higher price than their F1 option, namely Checkpoint model 2200 and Juniper model SRX550, while Cisco kept the same firewall, ASA5545, as the best option.

Checkpoint’s cheapest alternative for F1 has a significant difference in price compared to firewalls from other competitors, it is almost 66% cheaper than Juniper’s firewall and 75% cheaper than Cisco’s firewall. However, Checkpoint’s solution, firewall 2200, matches the requirement for new connections per second with the exact same value, i.e., there is no possibility for an improvement. However, if the next best firewall is chosen from Checkpoint, the 3100 model, it is still cheaper than the other two vendor’s alternatives. Checkpoint could also provide a good price alternative for F2 with the 5200 model, which price is 25% lower price than Cisco and 46% lower than Juniper’s model. Model 5100 also meets all the requirements, however its price is not mentioned in the considered documentation. Checkpoint’s alternative, model 5200, again fulfils the requirements with the exact required value, i.e., 20 virtual instances. Next best firewall is the 4800 model with 25 virtual instances and a higher price than both Juniper and Cisco have. As explained before, the price is only for the initial purchase, other fees related to a subscription or maintenance are not included. Based on an additional input from NNS labs report showing a price per protected data, Checkpoint can be seen as the best alternative.

As each vendor had a number of firewalls that satisfy all the requirements, the best option from each vendor was chosen by using the lowest listed firewall price. This might not be the best way of making a decision considered limitations of the work, however in these circumstances it is believed to be a reasonable decisive factor. Based on it, the best firewall from each vendor is presented in the comparison in tables 9 and 10.

Once the best firewall solution from each vendor has been chosen, the best solution among them also needs to be chosen. Looking at the price, Checkpoints options, model 2200 and 5200 are the best for both F1 and F2. If one considers possible future expansion of the network to any degree, Checkpoint still comes ahead for F1, however surpassed by both Juniper SRX3400 and Cisco ASA5545 as the cheapest solution on F2. Using the same vendor for both solutions can be a good idea as there are differences between the vendors configuration and user interfaces which can ease equipment usage. If we recognize a request of having the same vendor and favour the possibility of future expansion, Cisco with ASA5545 is the best solution with a thin margin.

10 Conclusions
In this thesis different firewall are investigated in order to find the best suited firewall for a specific network. With the use of requirements and metrics firewalls from three different manufacturers have been investigated and compared. From each of considered manufacturer a firewall that fulfils the requirements and has the lowest price is selected. Next, the selected firewalls from different vendors are compared between each other in order to find the best suited firewall for the specific network.
The specific network is a use case considered in this work coming from Eskilstuna municipality. Based on their network demands and literature review, relevant requirements were derived. Related metrics were identified for every requirement. The metrics are firewall functions or features through which requirements can be fulfilled. The metrics are used for conducting the comparison and for identifying the best suitable firewall.

Based on the use case, two options regarding firewalls placement were investigated through the comparison, one considered firewall was placed on a border of the network and one placed inside the network. The two firewalls have different requirements and, consequently required separate comparisons.

For the border firewall the result of the evaluation are showing that among Checkpoint’s products, the model 2200 is the best option. This firewall meets all the requirements and has the cheapest price. Juniper’s model SRX550 comes out as the best solution from Juniper, and ASA5545 model is best provided by Cisco. By comparing the identified three solutions from each vendor it was noted that the price for Checkpoint 2200 is three times less than Juniper SRX550 and four times less than Cisco ASA5545 prices. The Juniper and Cisco firewalls have higher performance capacity, however since Checkpoint 2200 satisfies all the requirements it is seen as the best solution for the border firewall.

The inside firewalls comparison results have a few differences compare to the border firewall evaluation results caused by a different set of related requirements. Cisco fulfils all the requirements with the same model, ASA5545, for the inside firewall as well as for the border firewall. Checkpoint’s model 5200 was identified as the best suitable option from Checkpoint, SRX3400 is in turn the best solution provided by Juniper. The price difference is less significant than for the border firewalls solution, though for this case Checkpoint again has the cheapest solutions that are three quarters cheaper than Cisco solutions and almost twice cheaper compare to solutions from Juniper. Therefore, Checkpoint’s solution, model 5200, can be regarded as the best solution for the inside firewall within limitations of the this work mentioned before and the considered use case.

The methods created in this thesis to compare the different firewalls can also be used in similar studies. The parameters used in the comparison are only valid for a specific network, other implementation of the method should therefore include parameters derived from that network case. Other parameters that have not been used in this thesis can include wireless, VPN, routing, throughput based on traffic and throughput with different security solutions turned on.
References

[16] NSS Labs, Inc., Test Methodology – Next Generation Firewall v7.0, Austin, TX 78746 USA, 2016.


